Security

Help Documentation

Security

Anti-Virus Administration

From this page you can enable SmarterMail to work with virus scanners that support a quarantine directory. SmarterMail has the ability to check the quarantine directory and respond to users who attempted to send an email containing a virus.

To get started, click the Security button on the main toolbar, then select Anti-Virus Administration from the Email Protection folder tree view.

Options

Enable ClamAV - Enable this to use ClamAV anti-virus scanning.

Enable Real-Time AV - Enable this to use Real-Time AV

Enable Command-Line AV - Enable this to use a command line virus scanner.

ClamAV

Clam AntiVirus is a 3rd party open source anti-virus toolkit, designed especially for scanning e-mail on mail gateways. For more information on ClamAV, visit: www.clamav.com

IP Address - The IP address of the ClamAV server to use.

Port - The Port that the ClamAV server is listening on.

Timeout (in seconds) - System Admins can enter the maximum number of seconds they want to wait before moving on. (Default is 10 seconds)

Failures Before Restart - System Admins can enter the maximum number of timeouts allowed before ClamAV is restarted. (Default is 5)

Virus Definitions - Displays when the virus definitions were last updated. The definitions are updated whenever the service starts and every 6 hours thereafter. Click the Update link to do an immediate update.

Real-Time AV

Quarantine Directory - Enter the full path to the quarantine directory set for the server.

Virus Action - Choose the action to be taken when an email contains a virus. The available options are shown below.

- Delete (Recommended) - This option will enable the SmarterMail service to delete any associated files attached to the message from the spool directory. This does not take any action on the quarantine directory.
- Inform Sender - This option will inform the 'From' address that a message was receive by the server, and because a virus was found in the message, it did not reach the intended recipient. Note: With some of the more recent viruses, this action becomes less useful, as many viruses now spoof the 'from' email address.

Command Line AV

Command Line - Enter the command that you want to execute. %FILEPATH will be replaced with the path to the file to be scanned.

Anti-Spam Administration

SmarterMail's anti-spam features allow you to be as aggressive as you want when combating spam.

To get started, click the Security button on the main toolbar, then select Anti-Spam Administration from the Email Protection tree view.

- Spam Checks - Check the spam options that you want to enable for filtering (a point-based weighting system for filtering spam) and for blocking at the SMTP level. Weights can also be edited for the various checks from this tab.
- Filtering - Choose the default weight thresholds and actions for various spam levels for filtering. Users can override these settings if you permit them to.
- SMTP Blocking - Set the weight to use as a threshold on this tab. Enabling this option will block email at the SMTP delivery level if too many spam checks fail.
- Options - This tab contains options relating to the processing of spam and overridability.

In short, when an email comes in, spam checks are run on it. The checks that fail add points to the email, which then put the email into a category of spam probability.

Spam Checks

Due to the flexible nature of SmarterMail's Anti-Spam setup, spam checks can influence the spam decision as much or little as you want. When spam protection runs on a particular email, all enabled spam checks are performed on the email. The total weight of all failed tests is what comprises the spam weight for the email. A spam probability level is then assigned to the email using the settings in the Filtering tab.

Note: Only enabled spam checks are used when calculating spam weight. To enable or disable a check, click on the appropriate checkbox next to it and click the Save icon.

The different types of Spam Checks are shown below. In most cases, clicking on the Edit icon will allow you to set various properties about it.

Declude

Declude integration allows you to use Declude products in conjunction with the SmarterMail weighting system. Declude addresses the major threats facing networks, and are handled by a multi-layered defense. Configuration of Declude is done through the Declude product, and all you need to do in SmarterMail is enable the spam check. Declude score will be included on spam line. Declude is a 3rd party open source and more information can be found at: www.declude.com .

SpamAssassin

SpamAssassin is a powerful, 3rd party open source mail filter used to identify spam. It utilizes a wide array of tools to identify and report spam. More information about SpamAssassin can be found at: spamassassin.apache.org .

SmarterMail includes a Windows version of SpamAssassin out of the box. By default, SmarterMail will run a version of SpamAssassin on 127.0.0.1 port 783. The System Administrator can enable and disable SpamAssassin by clicking the Security button on the main toolbar, then selecting SpamAssassin Servers from the Email Protection folder tree view. The Windows Version of SpamAssassin is limited to about 40,000 messages per day, if you anticipate more than this you may require the use of a distributed, multi-threaded version. Additional information is available in the SmarterTools SpamAssassin Deployment Guide.

SmarterMail can use SpamAssassin with its weighting system. By default SpamAssassin will run on 127.0.0.1:783. Additional servers can be setup from the Security->SpamAssassin menu option.

Low Probability of Spam - The weight that will be assigned if SpamAssassin determines a low probability of spam.

Medium Probability of Spam - The weight that will be assigned if SpamAssassin determines a medium probability of spam.

High Probability of Spam - The weight that will be assigned if SpamAssassin determines a high probability of spam.

Timeout - The timeout that SmarterMail will impose on a server if it cannot connect.

Maximum Attempts per Message - This will designate how many times SmarterMail will attempt to acquire a SpamAssasasin score before it gives up on that email.

Custom Headers

Email can be assigned spam weight based on headers in the message. Use this selection to configure weights for custom headers.

Header - The custom header to search for in the e-mail message.

Value - The value of the custom header.

Weight - The amount to add to the e-mail message's spam weight.

Bayesian Filtering

Bayesian Filtering uses statistical analysis to identify whether or not an email appears to be spam. Bayesian Filtering "learns" from previous spam-marked messages to progressively improve performance. Tying it together with blacklists and SPF allows you to be quite sure that email is or is not spam.

Weight - The default weight for this spam check. If an email has a high probability of being spam based on its content, this is the value that will be added to the message's total spam weight.

Max memory to allocate for filtering - Bayesian Filtering can be memory intensive. As a result, SmarterMail allows you to configure the maximum resources that will be dedicated to Bayesian Filtering. In general, the more memory you reserve for Bayesian Filtering, the more accurate the results will be.

Messages required for filter update - Once this number of messages have been processed as known-good or known-spam email, SmarterMail will re-analyze the filters to help your system protect against new spam threats. In this way, Bayesian Filtering can become more tailored to handle the mail of the domains on the server.

DomainKeys

DomainKeys is an e-mail authentication system designed to verify the DNS domain of an e-mail sender and the message integrity. The DomainKeys specification has adopted aspects of Identified Internet Mail to create an enhanced protocol called DomainKeys Identified Mail (DKIM).

SPF (Sender Policy Framework)

SPF is a method of verifying that the sender of an email message went through the appropriate email server when sending. As more and more companies add SPF information to their domain DNS records, this check will prevent spoofing at an increasing rate.

Pass - Indicates that the email was sent from the server specified by the SPF record (more likely good mail). The weight you set may be 0 (for no effect) or a negative number, thereby reducing the spam rating.

Fail - Indicates that the email was sent from a server prohibited by the SPF record (highly likely spam). Set this to a relatively high weight, as the probablility that the email was spoofed is very high.

SoftFail - Indicates that the email was sent by a server that is questionable in the SPF record. This should either be set to 0 or a low spam weight.

Neutral - Indicates that the SPF record makes no statement for or against the server that sent the email. Except in very special circumstances, leave this set to 0.

PermError - Indicates that there is a syntax error in the SPF record. Since SPF is relatively new, some domains have published improperly formatted SPF records. It is recommended that you leave this at 0 until SPF becomes more widely adopted.

None - Indicates that the domain has no published SPF record. Since SPF is relatively new, many legitimate domains do not have SPF records. It is recommended that you leave this at 0 until SPF becomes more widely adopted.

Reverse DNS (Domain Name Sever)

Reverse DNS checks to make sure that the IP address used to send the email has a friendly name associated with it.

Weight - The default weight for this spam check. If an email sender does not have a reverse DNS entry, this is the value that will be added to the message's total spam weight.

RBL Lists (Real-Time Blacklists)

RBL Lists (also known as IP4R Lists) are publicly accessible lists of known spammer IP addresses. These lists can be a very important part of spam protection. To attach to a list, click on the Add List icon. Some common RBL lists are shown at the bottom of this topic.

Name - A friendly name for the list that will help you and your customers identify it.

Weight - The default weight for this spam check. If an email sender is listed with the spam list, this is the value that will be added to the message's total spam weight.

DNS Server - Spam lists operate through DNS. As a result, each list provider gives out a DNS server that contains the blacklist. Enter it in this box.

Description - This field allows you to store additional information about the list.

Filtering

Emails are filtered into one of four categories based on their total weight. If a weight is equal to or higher than a certain category, then it is assigned that probability of being spam. Use the Actions tab to define the weight thresholds and the default actions at each level.

Weight Threshold - The email is sorted into probability levels based on the weight threshold values.

Action - The action to take when a message ends up with this probability.

Text to Add - This is the text that will be displayed when a message reaches a particular level of spam.

SMTP Blocking

This tab allows you to set up extra spam checks that block emails at delivery if a certain amount of spam checks fail.

Incoming Weight Threshold - Enable this and an incoming email must score this value or higher in order to be blocked. The score is established by the settings on the Spam Checks tab. (Default is 30)

Outgoing Weight Threshold - Enable this and an outgoing email must score this value or higher in order to be blocked. The score is established by the settings on the Spam Checks tab. (Default is 30)

Options

Auto Responders - Allows you to restrict what types of auto-responses are permitted for the system. Certain anti-spam organizations are starting to block those servers that auto-respond to spam traps. To reduce the possibility of this occurring, set the auto-respond option to be as restrictive as your clients will permit.

Content Filter Bouncing - As with auto-responses, certain anti-spam organizations also blacklist those servers that send bounce messages back to spam trap accounts. SmarterTools recommends setting this option to be as restrictive as your clients will allow.

Enable domains to override filter weights and actions - Many domain administrators have their own opinions on what spam checks work best for their domain. Enable this to allow them to override the spam options if they wish.

Enable bounces for Outgoing SMTP Blocking - Enable this to give a user a notification when a mail message has not been sent due to spam.

Enable Spool Proc Folder - Enable this to have SmarterMail place messages into this folder to be analyzed in the background. While the messages are in the Spool Proc folder, .hdr can manipulate

elements of the message, such as edit, write, and add headers. Once the scan has been completed, the message will be placed back into the spool and handled by SmarterMail from that point on.

Disable spam filtering on intra-domain email - Check this to disable spam filtering when messages are sent from from within the same domain (e.g. user1@example.com to user2@example.com).

Disable spam filtering on SMTP whitelisted IP Addresses - Check this to disable spam filtering on IP Addresses which have been added to a whitelist.

Enable Catch-All accounts to send auto-responders and bounce messages - Enable this if you rely on auto-responders being sent when a message comes in through a catch-all. In general, this is a bad idea, so it should be left unchecked unless your situation specifically requires it.

Bypass Gateways

This tab gives administrators the ability to enter an IP Address or an IP Range of an incoming gateway. SmarterMail will analyze the .EML file and pull the most recent IP Address from the header which will usually be an organizations incoming gateway. By inputting that IP Address on this page will allow SmarterMail to analyze the IP of the originating server rather than focusing on the gateway that SmarterMail received the message from. This is important because the majority of the time an organizations incoming gateway will not be listed on any RBL lists, but the originating server may be.

To add an IP Address or IP Range, click the Add IP icon from the Actions toolbar.

Blacklist / Whitelist

From this page you can control which IP addresses are blacklisted (not allowed) from mail services on this machine, or whitelisted (trusted) to access the mail services on this machine.

To get started with Blacklists, click the Security button on the main tool bar, then select Blacklist from the Security folder tree view.

To get started with Whitelist, click the Security button on the main tool bar, then select Whitelist from the Security folder tree view.

Note: Whitelisted IP addresses are not subject to relay restrictions which you may have imposed. Exercise caution when granting whitelist status to a server, and be sure that you know what services on that server may send mail through your server.

New icon - Click on this button to add an IP address or an IP address range to the list.

Edit icon - Click on a row to edit the whitelist or blacklist settings for the entry.

Delete icon - Click on this link to remove an entry from the list.

Adding / Editing an Entry

IP Address - Enter a single IP address in dotted quad notation (X.X.X.X) in this box if you want to add only a single IP (ex: 192.168.1.26).

IP Range - Enter a range of IP addresses in the two boxes, and all IP addresses that are contained in the range will be added (ex: 192.168.1.1 - 192.168.1.255).

Blacklist or Whitelist SMTP / POP / IMAP / Greylisting - Check the boxes for the protocols you wish to include in the blacklist or whitelist entry. The Greylisting checkbox is only available for whitelisted IPs, and if checked, the whitelisted IP will not be greylisted.

Abuse Detection

SmarterMail has several methods of preventing abuse and Denial of Service (DoS) attacks. The ones that can be configured are explained below. Any number of detection methods can be added.

To get started, click the Security button on the main toolbar, then select Abuse Detection from the Security folder tree view.

Once you arrive on the Abuse Detection screen, you will see three icons on the actions toolbar— New , Edit , and Delete .

When clicking the New icon on the actions toolbar you will have these options:

Denial of Service (DoS) Prevention - Too many connections from a single IP address can indicate a Denial of Service (DoS) attack. Enable this option to block IPs that are connecting too often to the server. It is recommended that you whitelist any trusted IP addresses that may send out large mailing lists or make many connections if you enable this option.

- Service Type - Select the service that will be monitored for this type of attack (POP/SMTP/IMAP/LDAP).
- Time Frame - The period of time in the past that is examined to determine if an IP address should be blocked. Too many connections in this period of time, and a block will be initiated.
- Connections Before Block - The number of connections before a block is placed. It is common for several connections to be open at once from an IP address. Set this to a relatively high value so that you can catch DoS attacks while not impacting legitimate customers.
- Time to Block - The number of minutes that a block will be placed once an IP hits the threshold.

Bad SMTP Sessions (Email Harvesting) - A bad session is any connection that ends without successfully sending a message. Many bad sessions usually indicate spamming or email harvesting.

Leaving all of these options set to 0 (zero) will disable this type of abuse detection. It is recommended that you whitelist any trusted IP addresses that may send out large mailing lists if you enable this option.

- Time Frame - The period of time in the past that is examined to determine if an IP address should be blocked. Too many bad sessions in this period of time, and a block will be initiated.
- Bad Sessions Before Block - The number of bad sessions before a block is placed. A few bad sessions happen once in a while, for instance when a person sends an email to an email account that does not exist. It is not these people that you are targetting, but rather those that are attempting to compromise or harass your customers.
- Time to Block - The number of minutes that a block will be placed once an IP hits the threshold.

Internal Spammer Detection and Notification - Enabling this feature in SmarterMail will alert an administrator whenever a multiple emails are received on the server of the same size.

- Time Frame - The period of time in the past that is examined to determine if an alert should be sent. Too many duplicate emails in this period of time, and an alert will be sent.
- Messages Before Notify - After this many duplicate messages are received within the time period specified, the email notification is sent.
- Email to Notify - The administrator account to which the notification will be sent.

Edit Icon - Editing and item can be done three ways:

- Select the item and then choose the Edit icon from the actions toolbar, or
- Right-click the item and choose Edit from the drop down list, or
- Double-click the item you would like to edit

Delete Icon - Deleting an item can be done two ways:

- Select the item and click the Delete icon from the actions toolbar, or
- Right-click the time and select Delete from the drop down list

Greylisting

What is Greylisting and how does it work?

Greylisting is a new tool in the fight against spam. It will temporarily block incoming mail from a sender and then returns the mail to the sender's mail server with a message saying effectively, "try again later." The sending server must then retry sending the mail after the Block Period but before the Pass Period (see below for definitions of these values).

Greylisting is effective because spammers will not usually bother to attempt a second delivery, but legitimate e-mail servers will.

Why use Greylisting?

Greylisting is a very effective method of spam blocking that comes at a minimal price in terms of performance. Most of the actual processing that needs to be done for Greylisting takes place on the sender's server. It has been shown to block upwards of 95% of incoming spam simply because so many spammers don't use a standard mail server which would do automatic retries.

How do I set up Greylisting?

Note: You must be a system administrator to change Greylisting settings.

In order to set up Greylisting, click the Security button on the main toolbar, then select Greylisting from the Email Protection folder tree view.

- Block Period - The period of time (in minutes) that mail will not be accepted (default 15 minutes).
- Pass Period - The period of time (in minutes) in which the sender's mail server has to retry sending the message (default 360 minutes).
- Record Expiration - The period of time(in days) that the sender will remain immune from greylisting once it has passed (default 36 days).
- Enable Greylisting - If this is enabled it will allow Greylisting to happen.
- Enable Users to Override Greylisting - Enable this to allow users to selectively turn off Greylisting (useful if you have an account that receives time sensitive mail).
- Enable Greylisting to SmartHosts - If this feature is enabled, it will determine whether or not SmartHosts are governed by Greylisting. This is determined by evaluating the MX record of the recipient's address and matching it against the IP address of any target server IP address configured in the SmartHost settings area. For more information, see the SmarterHosts section of the online help. System administrators should note that the following cases are exempt from Greylisting:

- Whitelisted IPs for SMTP or Greylisting
- Anyone who authenticates (includes SMTP Auth Bypass list)
- Trusted senders
- Anyone who has already sent you an email
- Any IP in the greylistBypass.xml file

Disadvantages of Greylisting

The biggest disadvantage of Greylisting is the delay of legitimate e-mail from servers not yet verified. This is especially apparent when a server attempts verify a new user's identity by sending them a confirmation email.

Some e-mail servers will not attempt to re-deliver email or the re-delivery window is too short. Whitelisting can help resolve this.

SpamAssassin

What is SpamAssassin and how does it work?

SpamAssassin is a powerful, free mail filter used to identify spam. It utilizes a wide array of tools to identify and report spam. These include:

- Header and text analysis
- Bayesian filtering
- DNS blocklists
- Collaborative filtering databases

When should you use SpamAssassin?

You should use SpamAssassin when you care about limiting spam from getting to your mailbox but cannot afford a high priced spam solution.

How do I set up SpamAssassin?

SmarterMail includes a Windows version of SpamAssassin out of the box. By default, SmarterMail will run a version of SpamAssassin on 127.0.0.1 port 783. The System Administrator can enable and disable SpamAssassin by clicking the Security button on the main toolbar, then selecting SpamAssassin Servers from the Email Protection folder tree view. The Windows Version of SpamAssassin is limited to about 40,000 messages per day, if you anticipate more than this, then please read our Anti-Spam Administration page from the Security folder in the Systems Administration section of the help files.

SMTP Blocked Senders

The SMTP Blocked Sender list is an effective method for temporarily canceling a domain or indiviual user's ability to send email on the server. For example, if a particular account is sending an abnormal amount of email, you can add their address to Blocked Senders and they will be unable to send email until you remove them from the Blocked Senders list. Users and/or domains can be left on the list for

whatever time you deem appropriate, and can be an effective stop-gap versus actually deleting the user and/or domain from the server.

To get started, click on the Security button on the main toolbar, then select SMTP Blocked Senders from the Security folder tree view.

Blocked Senders - Enter the email addresses or domain names you want to block, one per line. The asterisk (*) wildcard symbol is permitted in the list.

Forwarding BlackList

Emails cannot be forwarded to the domains in this list. This is to prevent issues with companies that have strict spam policies and blacklist the sending server for forwarded spam.

The most common instance of needing this feature is AOL * , which blacklists servers that forward spam to their servers. If this becomes a problem, you may decide to add AOL.com to your forwarding blacklist.

*AOL and AOL.com are registered trademarks of America Online, Inc.

SMTP Authentication Bypass

SMTP Authentication is a security measure that can be very beneficial in the fight against spam and unauthorized email. Unfortunately, some applications do not have support for SMTP authentication when sending mail. Most often, these are web sites that have automated mail sending mechanisms.

The solution is to add the IP addresses of the servers/sites to SmarterMail's SMTP Authentication Bypass. Any IP address entered into this page will not be asked to provide an SMTP Authentication login. In this list you can see all IP addresses that are bypassing SMTP Authentication.

To get started, click the Security button on the main toolbar, then select SMTP Authentication Bypass from the Security folder tree view.

New Icon - Click on this button to add additional IP addresses to the bypass. More information can be found below.

Edit Icon - Editing and item can be done three ways:

- Select the item and then choose the Edit icon from the actions toolbar, or
- Right-click the item and choose Edit from the drop down list, or
- Double-click the item you would like to edit

Delete Icon - Deleting an item can be done two ways:

- Select the item and click the Delete icon from the actions toolbar, or
- Right-click the time and select Delete from the drop down list

Adding a Bypass

IP Address - Enter a single IP address in dotted quad notation (X.X.X.X) in this box if you want to bypass only a single IP (ex: 192.168.1.26).

IP Range - Enter a range of IP addresses in the two boxes, and all IP addresses that are contained in the range will be bypassed (ex: 192.168.1.1 - 192.168.1.255).

SSL

This page is available in Enterprise Edition only

SmarterMail allows System Administrators to add Secure Socket Layer (SSL) and Transport Layer Security (TLS) rules.

To get started click the Security button on the main toolbar, then select SSL from the Security folder tree view.

When adding a new rule there are several fields that need to be addressed. These fields are:

IP Address - This is the IP address where SmarterMail will listen.

SMTP, POP, IMAP - Determines on which port SmarterMail will listen for the respective protocol.

Type - Sets the type of rule you would like to add, SSL or TLS. SSL always assumes the connnection will be secure, and therefore, sends the encryption immediately. TSL connects normally, and then looks to see if the connection is secure before sending the encryption.

Certificate Path - The path to the certificate file on the server. Typically, named a *.cer file.

- The certificate you are using must be added to the Certificates Microsoft Management Console within your Windows operating system. In addition, you must associate the Private Key with this same certificate.

Please Note: When removing a SSL rule, the System Administrator will need to perform a service restart.

Edit Icon - Editing and item can be done three ways:

- Select the item and then choose the Edit icon from the actions toolbar, or
- Right-click the item and choose Edit from the drop down list, or
- Double-click the item you would like to edit

Delete Icon - Deleting an item can be done two ways:

- Select the item and click the Delete icon from the actions toolbar, or
- Right-click the time and select Delete from the drop down list

Password Requirements

Minimum Password Length - This will allow System Administrators to designate the minimum numbers of characters a password requires.

Password Strength Requirements - The System Administrator is able to set the requirements for passwords and, as a result, all users must adhere to those standards. The password options available to the System Administrator are: Number, Capital Letter, Lower Case Letter, Symbol, Not User Name.